November 2010

MONTHLY Cyber Security Newsletter

Security Tips

Mississippi Department of Information Technology Services

Division of Information Security

This issue…

This month's newsletter provides information about Online Holiday Shopping Security. Keep the cyber Grinch away this season!

Key Term…

Known as **Cyber Monday**, the Monday after Thanksgiving is often the biggest online shopping day of the year. But it's not just online retailers hearing the "ka-ching" of virtual cash registers. Cyber criminals will also be banking on users' eagerness to get the lowest deals on Cyber Monday with a slew of scams and malware attacks designed to part shoppers from their credit card numbers.

Online Holiday Shopping Security Tips

Online shopping during the upcoming holiday season is expected to grow from last year, with one survey indicating 69 percent of respondents will be purchasing holiday gifts online, up from 64 percent in 2009. Faster Internet access speeds, coupled with enhanced functionality and deployment of mobile devices are just a few factors that may contribute to consumers' increased use of the Internet for holiday shopping. Before going online, however, it's important to understand the potential security risks and what precautions to take.

The following tips are provided to help consumers stay safe while shopping online using their personal computing device:

- ***Secure your computer.*** Make sure your computer has the latest security updates installed. Check that your anti-virus and anti-spyware software are running properly and are receiving automatic updates from the vendor. If you haven't already done so, install a firewall before you begin your online shopping.
- ***Upgrade your browser.*** Upgrade your Internet browser to the most recent version available. Review the browser's security settings. Apply the highest level of security available that still gives you the functionality you need.
- ***Secure your transactions.*** Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted. Also look for a broken key symbol indicating a non-secure connection. Some browsers can be set to warn the user if they are submitting information that is not encrypted.
- ***Be wary of potential scams.*** If the online offer sounds too good to be true, it probably is. Cyber criminals will look to take advantage of the volume of online shoppers to temp users to fall prey to online scams.
- ***Use strong passwords.*** Create strong passwords for online accounts. Use at least eight characters, with numbers, special characters, and upper and lower case letters. Don't use the same passwords for online shopping websites that you use for logging onto your bank, home or work computer. Never share your login information with anyone.
- ***Do not e-mail sensitive data.*** Never e-mail credit card or other financial/sensitive information. E-mail is like sending a postcard and other people have the potential to read it. Beware of emails requesting account or purchase information. Delete these emails. Legitimate businesses don't solicit information through email.

It Can Happen To You…

According to The Norton Cybercrime Report: The Human Impact, some form of cybercrime has affected more than two-thirds of the Internet population. 65% of global respondents have been victims of cybercrime (viruses, online credit card fraud, and identity theft).

- ***Ignore pop-up messages***. Set your browser to block pop-up messages. If you do receive one, click on the "X" at the top right corner of the title bar to close the pop-up message.
- ***Do not use public computers or public wireless to conduct transactions.*** Don't use public computers or public wireless connections for your online shopping. Public computers could potentially contain malicious software that steals your credit card information when you place your order. Criminals could be monitoring public wireless networks for credit card numbers and other confidential information.
- ***Review privacy policies.*** Review the privacy policy for the website/merchant you are visiting. Know what information the merchant is collecting about you, how it will be stored, how it will be used, and if it will be shared or sold to others.
- ***Make payments securely.*** Pay by credit card rather than debit card. Credit/charge card transactions are protected by the Fair Credit Billing Act. Cardholders are typically only liable for the first $50 in unauthorized charges. If online criminals obtain your debit card information they have the potential to empty your bank account.
- ***Use temporary account authorizations*.** Some credit card companies offer virtual or temporary credit card numbers. This service gives you a temporary account number for online transactions. These numbers are issued for a short period of time and cannot be used after that period.
- ***Select merchants carefully.*** Limit your online shopping to merchants you trust. Confirm the online seller's physical address and phone number beforehand. If you have problems, concerns, or questions regarding a merchant, check with the Better Business Bureau or the Federal Trade Commission. Don't forget to review merchant's return policies to avoid product return issues.
- ***Keep a record.*** Keep a record of your online transactions, including the product description and price, the online receipt, and copies of every e-mail you send or receive from the seller. Review your credit card and bank statements for unauthorized charges.

If you have problems shopping online, contact the seller or site operator directly. If those attempts are not successful, you may wish to contact the following entities:

- The Attorney General's office in your state (www.naag.org)
- Your county or state consumer protection agency
- The Better Business Bureau at: (www.bbb.org)
- The Federal Trade Commission at: (www.ftc.gov)

For additional information about safe online shopping, please visit the following sites:

- US-CERT: www.us-cert.gov/cas/tips/ST07-001.html
- National Cyber Security Alliance: www.staysafeonline.org/in-the-home/online-shopping
- OnGuard Online: www.onguardonline.gov/topics/online-shopping.aspx
- Online Cyber Safety: www.bsacybersafety.com/video/
- Microsoft: www.microsoft.com/protect/fraud/finances/shopping_us.aspx
- Privacy Rights Clearinghouse: www.privacyrights.org/fs/fs23-shopping.htm#2

Keep the Cyber Grinch at Bay this Holiday Season!

AliceClaire Thompson

While many holiday shoppers have replaced the swiping of a credit card with a point and click on a computer screen, cyber criminals are becoming even more creative in their fraudulent ways to snatch your personal information. According to Internet Retailer, 72% of shoppers will buy some, if not all, of their holiday gifts online this season. With the surge in online holiday shopping comes the increase of opportunities for cyber criminals to create new and deceitful ways to capture personal information including: bank account information, Social Security numbers, passwords, and other sensitive data. This holiday season keep the cyber Grinch away by educating yourself on phishing and social engineering scams.

Becoming familiar with the following terms will better your understanding on cyber crime. Phishing is defined as the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Social Engineering is defined as the art of manipulating persons in order to bypass security measures and tools. The purpose is to obtain confidential information from users through phone, e-mail, or direct contact to obtain unauthorized access to sensitive and personal data. This information can be extracted verbally, as well, by someone impersonating a legitimate user of the information being requested.

Follow these tips to secure your identity and personal information this year:

- Be wary of emails that look as if they are from a legitimate organization requesting personal information. Trustworthy companies will not ask for this information via email. Contact the company mentioned in the email by a number you know to be valid or open a new browser and search for the company's web site directly. Phishers can create links that look genuine but will take you to a site where your information is captured as soon as it is entered.

- Don't email personal or financial information. Email is not a secure way of transmitting data. If you want to provide this information through a company's website, check for indicators that it's a secure site. Indicators would be a lock icon on the browser's status bar or a URL for the website that begins with "https" (the "s" stands for "secure").

- Keep your computer updated with the latest security updates. Use a firewall, whether it is a network appliance or a personal firewall software package, to strengthen your home network. Cyber criminals are constantly looking for vulnerabilities and weak links in home users systems. Network firewalls (whether software or hardware–based) can provide a barrier against these attacks. This shouldn't be your only action to secure your system, other security measures need to be taken into consideration and applied as well. Turn off your computer or disconnect its Ethernet interface when the computer is not in use.

- Create strong passwords for online accounts and change them frequently, at a minimum, every 90 days. According to a study done by StaySafeOnline.org, 33% of online users never change their passwords. When creating a password, use at least 8 characters with upper and lower case letters, numbers, and symbols. Use different passwords for online shopping than you use for logging onto your home network or signing into your email account.

Online Shopping Statistics

Research by Internet Retailer says that 72% of U.S. online consumers will shop online for holiday gifts this season. Surveys show that consumers are shopping online more often to avoid the crowds and long lines and also because it's easier to compare prices online. According to eMarketer.com, 46.7% of retail executives in America expect their holiday online revenues to increase by 10% this year. E-retail sales for November 1-21 totaled $9.01 billion, comScore says, 13% higher than $7.95 billion for the comparable three-week period last year.

this newsletter is brought to you by…

MS-ISAC

www.msisac.org

www.its.ms.gov/services_security.shtml

- Only buy from trusted online companies. If you cannot confirm that the site is legitimate or not, do not purchase from this site. Research companies that you are unsure about. Search engines will usually come back with any related scams, complaints, and warnings about the company, giving you more information to make a wise decision.

If you believe you've been a victim of identity theft, there are several ways you can fight back. You should notify the authorities about the fraud or identity theft. Contact the Federal Trade Commission (www.consumer.gov/idtheft) or 1-877-IDTHEFT. If you think you have been scammed, you can report the incident to the Internet Crime Complaint Center (www.IC3.com). This is a partnership between the FBI, the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance. This group only focuses on cyber-crime whether it is an internet scam, identity theft, or other acts of fraud. By reporting these incidents you are doing your part to help protect yourself and others from being victimized by cyber-crime. Protect yourself this holiday season by staying educated on current holiday phishing scams and stop the cyber Grinch from stealing your holiday spirit this year!

How Do I Know if it's a Scam?

If you are wary of an offer or a suspicious email, there are a few things you can do to research its validity.

- www.consumerfraudreporting.com
  - This site will give you information of top scams and cyber crimes and also provides a place to report an incident to aid in the prevention of it happening to someone else
- www.snopes.com
  - This site provides a multitude of scams and reports and informs you whether they are legitimate offers or if the information is part of a cyber criminal's plan to capture your sensitive information. It also compiles a list of the top 25 scams to be on the lookout for.
- www.google.com
  - One of the fastest ways to find out if an email or site is trying to scam you is by using a search engine to look for information. Provide the company's information and search for comments on their reputation from other users like you. More than likely if it's a fraud, someone is already talking about it and information will be available.

Remember: if it looks too good to be true, it probably is!